Elmlea Schools' Trust
Online Safety Policy

Document History Record of recent Policy changes

Date	Author/Owner	Change	Origin of
September 2021	Tom Weller		

Trustees 'Committee	Local Governing Body Joint Committee
Policy Adopted	October 2021
Review cycle	Annual
Review date	Autumn Term 2022

Contents

1. Aims

Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Elmlea Schools' community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Scope of Policy

This policy applies to all members of the Elmlea Schools' community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of schools' ICT systems, both in and out of the schools.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents (such as sending or receiving inappropriate images and messages) covered by this policy, which may take place outside of the school, but is linked to membership of the school.

When safeguarding issues arrise this policy will need to be used in conjunction with the safeguarding policy and anti-bullying policy. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 Governors

The governors have overall responsibility for approving and monitoring this policy and holding the headteacher to account for its implementation.

The governors will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on **acceptable use of the trust's** ICT systems and the internet (appendix 2)

3.2 The Head teacher and SLT

The headteacher is responsible for ensuring the safety of all members of the school trust's community. The day to day responsibility for online safety will be led by the Computing Lead.

The Head teacher will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks
- Support the Computing Leads by ensuring they have sufficient time, training and resources to fulfil their online safety responsibilities.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Will monitor communications on the home learning platform to check levels of appropriateness
- Will promote and monitor use of CPOMS for reporting safeguarding concerns

3.3 The designated safeguarding leads

Details of the school's designated safeguarding leads (DSL) are set out in our child protection and safeguarding policy.

The DSL's take lead responsibility for online safety in the schools, in particular:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the trust
- Working with the computing coordinator and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy
- Will monitor communications on the home learning platform to check levels of appropriateness
- Will promote and monitor use of CPOMS for reporting safeguarding concerns

3.4 The computing coordinator

The computing coordinator takes responsibility for the day to day online safety issues.

The computing coordinator will:

- Ensure that all staff are comfortable with reporting procedures following an online safety incident taking place.
- Maintain records of online safety concerns, as well as actions taken, as part of Elmlea Schools' Trust safeguarding recording mechanisms – including CPOMS
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Updating and delivering staff training on online safety
- Liaise with school technical staff
- Report regularly to SLT
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Will monitor communications on the home learning platform to check levels of appropriateness.

3.5 Technical staff

The Computing Coordinators along with technical staff within Elmlea Schools' Trust will:

- Conducting a full security check and monitoring of the school trust's ICT systems on a termly basis
- Ensuring that users only have access to suitable areas of the network and server
- Ensuring that the school trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Keep up to date with online safety technical information and to share this with others.
- Monitor usage of the network and internet so misuse can be identified and investigated

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school trust's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Implementing this policy consistently
- Teaching pupils to follow the policy and acceptable use policy correctly – particularly when discussing home learning platforms
- Teaching online safety lessons regularly following curriculum overview
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensuring digital communications with parents/carers should be on a professional level and only using school trust's systems
- Embedding online safety across the curriculum and other areas of school life
- Teaching pupils to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Teachers will model appropriate communication in all interactions with pupils.

3.7 Parents

Parents can play an important role in helping their children understand to navigate the digital world in an appropriate way. The school will support parents with parents' evening, newsletters and website updates with links to support.

Parents and carers will:

- Role model safe and appropriate use of technology and social media.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- read and ensure their child has read, understood and agreed to the terms on acceptable use of the school trust's ICT systems and internet (appendix 1)
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Monitor their children's' home learning platform and the response they give

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.8 Pupils

Pupils:

- are responsible for following the Pupil Acceptable Use Policy
- need to have a good understanding of safe searching, research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online Safety Policy covers their actions out of school, if related to their membership of the school trust
- must demonstrate their understanding of how to be a good digital citizen when using home learning platforms

3.9 Visitors and members of the community

Visitors and members of the community who use the school trust's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Education

4.1 Pupils

Elmlea Schools' Trust will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners.

Pupils will:

- Receive a broad online safety curriculum with staff reinforcing message across all areas of the curriculum whenever technology is in use
- Be helped to understand the acceptable use policy
- Be taught about keeping personal information private, use of passwords and online messaging.
- Have assemblies where key messages will be reinforced.
- Be involved in the creation of posters to promote the terms of the acceptable use policy.
- Be supported by vigilant teachers when using the internet to search freely.
- Learn how to be critically aware of materials the read and view and shown how to validate information
- Be asked for their views when writing and developing online safety policies and practices, including curriculum development and implementation.

4.2 Parents

The school trust will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website. High profile events such as Safer Internet Day will also be used to provide information and improve awareness for parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

4.3 Staff

Staff need to be confident with online safety to be able to implement this policy and support the education of all pupils with Elmlea Schools' Trust.

Staff will:

- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- Follow the guidance of the 'Education for a connected world'. And 'Keeping children safe in education' when planning our online safety curriculum
- Be updated through the Computing Leads on any relevant information or changes that would further their understanding of online safety.
- Be involved in discussions during staff meetings when the policy is updated
- Be supported by the computing leads when advice or guidance is required.

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

5. Technology

5.1 Infrastructure

The school will ensure that the infrastructure and network is safe and secure, and all areas identified in the policy are implemented.

- There will be regular reviews and audits of the safety and security of school trust's technical systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and Computing Leads and kept in a secure place.
- The Computing Leads, business manager and ICT service provider is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content is filtered by South West Grid For Learning (SWGfL)
- Request for filtering changes must go through the Headteacher/Technical staff.
- The school trust has provided differentiated user-level filtering (allowing different filtering levels for pupils/ staff/ visitors etc).
- Any technical incidents/ security breaches should be made known to the ICT service provider as soon as they are known.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school trust's systems and data. The school trust's infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6.2 Technology used

The range of technologies used in Elmlea Schools' Trust includes (but is not limited to):

- Laptops
- PCs
- Ipads
- The internet
- Social media platforms/home learning platforms
- Digital cameras

6.3 Managing filtering

The ICT Co-ordinators will manage the permitting and banning of additional web sites identified by staff members as appropriate or inappropriate.

Elmlea Schools' Trust will work in partnership with parents/carers, Bristol City Council and the school trust's ICT service provider to ensure systems to protect children and young people are reviewed and improved.

If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (Bristol City Council) via the ICT Co-ordinator or the school's ICT service providor.

If a child discovers unsuitable content, their parents will be contacted immediately by teacher or other member of staff.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school trust or organisation believes is illegal must be referred to the Internet Watch Foundation (IWF - http://www.iwf.org.uk/) and Bristol City Council.

.

6.4 Data protection

Personal data will be recorded, processed, transferred and made available in line with our GDPR Data Protection policy.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school trust's behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school trust will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. This can be linked to the use of home learning platforms and interactions with other pupil's work.

In relation to a specific incident of cyber-bullying, the school trust will follow the processes set out in the school trust's behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school trust will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in the schools

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school trust's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school trust's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Mobile devices in the Junior School

Parents may seek permission of the Headteacher for their children to bring mobile phones into the Junior school. In these instances, the phones should be switched off and kept in Junior school bags whilst on Junior school premises.

Pupils are not permitted to use these devices for recording still or video images.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Junior school behaviour policy, which may result in the confiscation of their device.

Staff should secure their personal phone throughout the Junior School day – it should not be used in lesson time during a normal school day.

Staff should never use their personal phones to record or take photos of children.

This is not applicable at the Infant School Site

9. Staff using work devices outside the schools

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

Any USB devices containing data relating to the school must be encrypted.

10. How the school trust will respond to issues of misuse

Where a pupil misuses the school trust's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school trust's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed yearly by the computing lead. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- GDPR Data protection policy
- Complaints procedure
- Anti-bullying policy

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school trust's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- I will not look at, move or delete other people's files.
- I will not alter any settings or rename desktop items.
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer

If I bring a personal mobile phone or other personal electronic device within the school trust:

- I will not use it during lessons, clubs or other activities organised by the school trust, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- I will not take any photographs or videos when on the school trust premises without permission of the Headteacher.

I agree that Elmlea Schools' Trust will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that if I deliberately break these rules, I could be stopped from using the internet, computers or iPads.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school trust's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school trust's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school trust's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details • Take data out of school trust on removable storage such as USB sticks.	
I will only use the Elmlea Schools' Trust ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school trust will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person(s) who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**